

# Produktbeschreibung T.O. WebVPN

Stand: Juni 2005

V 1.0

Merkmale des  
T.O. WebVPN

### Was kann das T.O. WebVPN?

Das T.O. WebVPN basiert auf SSL-VPN-Technik und ermöglicht den Zugriff auf interne Ressourcen wie Webanwendungen (z. B. Intranet), Dateiserver (z.B. Samba) oder netzbasierte Software (z.B. ERP-Systeme). Dabei kann man verschiedenen Benutzergruppen unterschiedliche Zugriffsrechte zuweisen. Das T.O. WebVPN erfüllt Anforderungen an die EDV, für die man sonst hohe Investitionen und viel Know-how aufwenden müsste: Sie sparen sich die Installation spezieller Software auf den PC-Arbeitsplätzen und erhöhen Ihre Sicherheit. Anders als beim IPSEC- oder L2TP-VPN benötigen Sie für die Nutzung des T.O. WebVPN lediglich einen Webbrowser. Die Verbindung mit Ihrer webbasierten Anwendung erfolgt nach Authentifizierung mit einem Einmalpasswort verschlüsselt über unsere zentrale SSL-VPN-Infrastruktur und ist damit sicher gegen Angriffe von außen geschützt.

Begriff des SSL-VPN

### Was ist überhaupt ein SSL-VPN?

„SSL-VPN“ ist ein Marketingbegriff für die Kombination verschiedener Zugriffstechniken von außen auf firmeninterne EDV-Ressourcen. Der bereits eingeführte Begriff des „virtuell privaten Netzwerks“ VPN steht für die Nutzung öffentlicher nicht abhörsicherer Leitungen zur Übertragung vertraulicher Daten, wobei die Anwendung von Verschlüsselung so genannte „Tunnel“ durch das öffentliche Netzwerk – im Allgemeinen das Internet – legt. Man unterscheidet dabei zwischen standortverbindenden Tunneln („Site-to-Site-VPN“), welche den Einsatz teurer und meistens schmalbandiger Standleitungen überflüssig machen, und Fernzugriff auf interne Daten durch Tunnel mobiler Benutzer in das Unternehmen („Remote Access VPN“).

Zugriff ohne spezielle  
Client-Software

Durch die SSL-VPN-Technik können mobile Benutzer auf interne Daten zugreifen, ohne dafür über spezielle Software verfügen zu müssen. Der Webbrowser (Mozilla, Firefox, Internet Explorer oder vergleichbare Software) dient dabei als universeller VPN-Client. Dies macht die Installation spezieller Software (IPSEC-Clients) auf den externen Clientrechnern überflüssig, welche im klassischen Fall zum Einsatz kommt. Der Einsatz des Webbrowsers erklärt so den Begriff SSL: „Secure Socket Layer“ wird seit mehr als 10 Jahren als Industriestandard unter anderem zum abhörsicheren Zugriff auf Webangebote per HTTPS genutzt (z. B. bei der Übertragung von Daten beim Online-Banking, Online-Shopping oder Webmail-Zugriff).

Universalclient  
Webbrowser

Zusammengefasst ist ein SSL-VPN (manchmal auch "clientless VPN" genannt) eine Technik für mobile Benutzer, um mittels eines Webbrowsers abhörsicher (durch SSL) auf interne EDV-Ressourcen zugreifen zu können (wie über ein VPN).

### Was macht man denn nun konkret mit dem T.O. WebVPN?

Dem Webbrowser als universellem VPN-Client ermöglicht das T.O. WebVPN nach erfolgreicher Anmeldung auf drei verschiedene Arten den Zugriff auf interne EDV-Ressourcen:

Webbasierte Informations-systeme per reverse Proxy

1. Interne webbasierte Informationssysteme (z. B. Webmail, Intranet, Kalender etc.) werden von außen erreichbar gemacht, in dem das SSL-VPN-Gateway als „reverse Proxy“ agiert: Die Zugriffe des mobilen Benutzers per HTTPS werden auf dem Gateway angenommen. Das Gateway verhält sich gegenüber dem internen Webserver als Client (diese Technik wird umgekehrt häufig beim Zugriff vom lokalen Netzwerk in das Internet in Form eines Proxy-Servers verwendet – daher der Name „reverse Proxy“). Hierbei werden alle internen Verweise (Links, Cookies, Skripte etc.) auf dem SSL-VPN-Gateway so umgeschrieben, dass ein externer Zugriff möglich ist.

So wird z. B. aus der Intranet-Adresse <http://televerzeichnis.firma.local/> die von außen nach Anmeldung am Gateway erreichbare Internet-URL <https://firma.webvpn.net/televerzeichnis/>.

Webzugriff auf Dateifreigaben

2. Interne Datenablagen (Windows-Netzwerkfreigaben bzw. exportierte Dateisysteme) können durch ein SSL-VPN-Gateway in Form einer Webseite von außen erreichbar gemacht werden. Dabei bereitet das Gateway die Sicht auf die internen Daten so auf, dass diese innerhalb des Browsers wie im Dateisystem bearbeitet werden können (Kopieren, Verschieben, neue Verzeichnisse anlegen etc.).

Selbstverständlich werden nur spezielle Freigaben von außen sichtbar gemacht, so dass mobile Benutzer z.B. den Zugriff auf Datenblätter haben oder Angebote von außen in das Netzwerk einstellen können.

TCP-Tunnel über Browser

3. Interne Netzwerkserver, die Dienste über TCP anbieten (z. B. Mailserver, Terminalserver, ERP-Systeme und ähnliches), können mittels eines über den Browser gestarteten Mini-programms (Java-Applet) mit Hilfe von TCP-Tunneln genutzt werden: Dieser stellt lokal installierten Anwendungen den internen Serverport über die SSL-Verbindung auf dem Client zur Verfügung. So werden spezielle interne Dienste von außen erreichbar gemacht und der Einsatz von Clientprogrammen ermöglicht. Über diesen Weg ist z. B. der sichere Zugriff auf interne E-Mail mit dem Mailclient möglich. Zudem wird die Technik häufig dafür eingesetzt, Terminalserver-Zugriff mit Microsoft-RDP- oder Citrix-ICA-Protokoll von außen zu ermöglichen, ohne IPSEC-Software einsetzen zu müssen.

### Wozu benötigt man starke Authentifizierung?

Voraussetzung starke Authentifizierung

Das T.O. WebVPN erfordert zwingend eine so genannte „starke Authentifizierung“ der mobilen Benutzer. Dies ergibt sich daraus, dass der Zugriff mittels Webbrowser von beliebigen Clients aus erfolgen kann. Die Sicherheit und Integrität dieser Rechner ist aber häufig vom Benutzer nicht beeinflussbar und muss daher als nicht gegeben vorausgesetzt werden (das betrifft insbesondere das Vorhandensein aktueller Updates, Virenschutz, korrekt aufgesetzte Firewall, Schutz gegen Spionageprogramme, Keylogger und vieles mehr). Aus diesem Grund wird beim Zugriff in das interne Netz ein Einwegpasswort verwendet, welches nur genau einmal die Anmeldung am T.O. WebVPN-Gateway erlaubt. Abgehörte, versehentlich gespeicherte oder mitgeschnittene Passwörter können daher nicht nochmals zum Anmelden verwendet werden.

Einwegpasswort auf Knopfdruck

Um den Benutzern den Umgang mit Einwegpasswörtern möglichst einfach zu machen, bekommen diese einen Passwortgenerator (Token), mit dem sie auf Knopfdruck ein Passwort generieren können. Dieses bildet zusammen mit einer nur dem Benutzer bekannten PIN den aktuellen Zugangscode analog dem gängigen Prinzip der Kombination des Besitzes (in Form des Tokens) und Wissens (in Form der PIN). Im Fall des Verlusts oder Diebstahls des Generators bzw. der PIN wird der Benutzer zentral am Authentifizierungsserver gesperrt und kann sich dann nicht mehr am T.O. WebVPN-Gateway anmelden.

Besitz und Wissen

### Wie funktioniert das T.O. WebVPN?

Einstiegshürde Investitionskosten

Der Aufbau eines SSL-VPN-Zuganges in die Firma erfordert neben einer nicht unerheblichen Investition in Hard- und Software das Wissen um die korrekte Installation, Konfiguration und Integration in die vorhandene EDV-Landschaft. Zudem muss die Verfügbarkeit im laufenden Betrieb sicher gestellt werden. Daher bietet Thinking Objects den Betrieb eines SSL-VPN in Form des T.O. WebVPN für kleine und mittelständische Kunden an, das alle Vorteile der Technik mit einer niedrigen Anfangsinvestition und fairen monatlichen Preisen kombiniert. Dabei werden alle externen Komponenten von T.O. betrieben und gewartet.

Komponenten T.O. WebVPN

Diese Komponenten sind

- ein hochverfügbares SSL-VPN-Gateway an einer leistungsfähigen Internet-Verbindung
- ein hochverfügbarer Authentifizierungsserver zur Anmeldung mobiler Benutzer
- ein Passwortgenerator in Form eines Schlüsselanhängers für jeden Benutzer und
- eine VPN-Verbindung vom Rechenzentrum der T.O. in das LAN der Firma basierend auf gängiger VPN-Hardware (klassische IPSEC-Tunnelverbindung).

Mit dieser Konstruktion werden die Daten zwischen den mobilen Benutzern und dem internen LAN durchgängig sicher verschlüsselt. Die internen Server werden lediglich vom SSL-Gateway über den IPSEC-Tunnel abgefragt. Es werden daher keine internen Dienste direkt im Internet exponiert.

#### Im Detail funktioniert das Ganze wie folgt:

Anmeldung mit  
Einwegpasswort

1. Der mobile Benutzer meldet sich von einem beliebigen Arbeitsplatz mit Internet-Anbindung mit dem Webbrowser an der Portalseite des SSL-VPN-Gateways an. Dazu übermittelt er einen Benutzernamen und das aktuelle vom Passwortgenerator angezeigte Kennwort zusammen mit seiner persönlichen PIN.

Authentifizierung

2. Das SSL-Gateway übermittelt die Anmeldedaten an den Authentifizierungsserver. Dieser prüft, ob das eingegebene Passwort gültig ist und meldet den Erfolg oder Misserfolg an das Gateway zurück.

Autorisierung

3. Eine erfolgreiche Anmeldung führt den Benutzer nach dem Start einer zusätzlich integrierbaren Kontrolle des Arbeitsplatz (z.B. Virenschutz oder Firewall vorhanden) auf die Einstiegsseite. Von diesem virtuellen Arbeitsplatz aus sind alle webbasierten Anwendungen und freigegebene Dateisysteme mit einem Mausklick erreichbar. Die Freigaben können vom Ergebnis der Kontrolle des zugreifenden Clients abhängig gemacht werden.

Aufbau TCP-Tunnel

4. Falls TCP-Tunnel aufgebaut werden, kann der Benutzer nun auch mit lokal installierter und speziell konfigurierter Software auf interne Serverdienste (Mailserver, Terminalserver, ERP-System o. ä.) zugreifen.

Abmeldung manuell  
oder automatisch

5. Die Verbindung wird vom Benutzer durch Abmeldung aktiv geschlossen oder nach Ablauf einer definierten Maximalzeit bzw. einer maximalen Leerlaufzeit automatisch invalidiert. Ein neuerlicher Zugriff ist dann nur durch Wiederanmeldung mit einem neuen Einwegpasswort möglich.

## Was sind die Vorteile des T.O. WebVPN?

Klare Vorteile und Sicherheit

Durch den Einsatz des T.O. WebVPN gewinnen Sie nicht nur einen einfachen Zugriff in Ihr Unternehmensnetzwerk, sondern auch eine Menge Sicherheit und Verfügbarkeit. Dabei benötigen Sie keine eigene Installation, sondern greifen über eine zentral verwaltete Infrastruktur auf von Ihnen freigegebene EDV-Ressourcen zu.

Schutz der Server

### 1. Keine direkte Erreichbarkeit Ihrer internen Server aus dem Internet:

Dies bedeutet, dass auch im Fall einer Sicherheitslücke auf einem Intranetserver (z. B. im IIS oder Apache) dieser Dienst von außen nicht angreifbar ist. Zudem werden Angriffe zur Unterbrechung des Dienstes („Denial-Of-Service“) wirkungsvoll verhindert.

Einwegpasswort

### 2. Zugriff auf interne EDV-Ressourcen von außen nur nach Anmeldung mit Einwegpasswort möglich:

Die Sicherheit ist damit wesentlich höher als bei Verwendung klassischer Passwörter, die ausgespäht, abgehört, mitgeschnitten oder abgespeichert werden können. Die Anmeldung bestimmt darüber hinaus, welche Ressourcen verwendet werden können, da diese den Benutzern gruppenweise und abhängig vom Endgerät geschaltet werden.

Durchgängig abhörsicher

### 3. Abhörsichere Übertragung der Daten vom mobilen Benutzer bis zum internen Server und zurück:

Mit SSL vom Benutzer zum SSL-VPN-Gateway und zusätzlich zwischen dem T.O.-Rechenzentrum und Ihrem Firmennetz per IPSEC verschlüsselten Verbindungen ist ein Abhören praktisch ausgeschlossen. Der VPN-Tunnel zwischen T.O. und Ihrer Firma wird zudem über Zertifikate authentifiziert und per Paketfilter auf beiden Seiten IP-technisch abgesichert.

Webbrowser oder Clientsoftware

### 4. Alle Vorteile der SSL-VPN-Technik können genutzt werden:

Der Zugriff per Webbrowser ist möglich auf webbasierte Intranet-Anwendung, Netzwerkfreigaben und TCP-Serverdienste. Auch der Einsatz eines speziellen SSL-Clients ist auf Wunsch möglich (lokale Installation auf dem mobilen Client wie z.B. dem firmeneigenen Notebook).

Durchgängig hochverfügbar

### 5. Hochverfügbarkeit durch Redundanzen:

Sowohl das SSL-VPN-Gateway, als auch der Token-Authentifizierungsserver, der VPN-Router im Rechenzentrum und die Internet-Anbindung sind durch Verdoppelung bzw. Backup-Konstruktionen hochverfügbar.

Überwachung Alarmierung

### 6. Überwachung der Verfügbarkeit:

T.O. überwacht die Erreichbarkeit des SSL-VPN-Gateways und Ihrer Serverdienste. Auf Wunsch werden Ihnen Alarmierungen zugesendet, wenn die von Ihnen angebotenen Dienste nicht mehr korrekt arbeiten oder gar nicht erreichbar sind.

### Wann sollte man das T.O. WebVPN einsetzen?

Webmail	– Sie betreiben einen im Internet erreichbaren Webmailserver (z. B. Outlook Web Access, Groupwise Web Access, Squirrelmail o.ä.) ohne starke Authentifizierung.
Dateizugriff	– Sie betreiben interne Dateiserver, auf denen Informationen zur Verfügung gestellt werden, auf die auch von Heimarbeitsplätzen, Außendienstmitarbeitern, Partnern oder bestimmten Kunden bequem zugegriffen werden soll.
Gemanagte Infrastruktur	– Sie wollen Zugriffe auf interne EDV-Ressourcen ohne Aufwand auf Seite des Clients und flexibel verwaltet zur Verfügung stellen, ohne dafür eine eigene Infrastruktur betreiben zu müssen.
Zugriff überall	– Sie wollen von überall per PDA und WLAN oder am Internet-Kiosk auf interne Webserver zugreifen und dabei das Abhören von Daten und Passwörtern verhindern.
Sicherheitsanforderungen	– Ihre Sicherheitsanforderungen sind so hoch, dass eine klassische Ankopplung des mobilen Clients per IPSEC-VPN nicht in Frage kommt, sondern ein Proxy zwischengeschaltet werden muss.
Fremdarbeitsplätze und Partnerzugriff	– Der Zugriff auf interne EDV-Ressourcen erfolgt über externe Arbeitsplätze, die nicht unter Ihrer Verwaltung stehen und auf deren Installation, Konfiguration und anderweitige Nutzung Sie keinen Einfluss haben.
Installation auf Fremdrechnern	– Ihre Administratoren verwenden viel Zeit auf das Ausrollen und regelmäßige Aktualisieren von VPN-Clientsoftware auf Rechnern, die nicht unter Ihrer administrativen Verantwortung stehen und demgemäß nicht nach Ihrem Firmenstandard installiert sind. – Mitarbeiter von Ihnen arbeiten bei Kunden in deren Netz und haben durch rigide Firewall-Regeln von dort keine Möglichkeit, ausgehende IPSEC oder L2TP-Verbindungen zu Ihrem Gateway zu öffnen. Der Zugriff auf das WWW per HTTPS ist aber möglich.

### Wie greift man auf das T.O. WebVPN zu?

Von jedem beliebigen Webbrowser aus verbindet man sich auf das Portal unter <http://firmenname.webvpn.net>. Von dort aus wird man automatisch auf die Anmelde-seite für die Firma weitergeleitet. Nach Eingabe von Benutzername, Einmalpasswort und PIN gelangt man auf den Portal-Arbeitsplatz, von wo aus alle internen Ressourcen im direkten Zugriff sind. Gegebenenfalls kann man dort auch Tunnelverbindungen aktivieren, die für einen Direktzugriff benötigt werden (zum Beispiel am Heimarbeitsplatz für den Terminaldienste-Client oder eine ERP-GUI).

Nach Ende der Sitzung meldet man sich vom Portal ab. Eine spezielle Software beseitigt alle Spuren auf dem verwendeten PC (Browsercache, Cookies etc.) und der Browser wird geschlossen. Damit ist die Sitzung unwiderruflich geschlossen und kann auch an öffentlich zugänglichen Terminals ohne Neuansmeldung nicht wiederhergestellt werden.

# Leistungsspektrum der Thinking Objects Software GmbH

Die Thinking Objects Software GmbH ist auf die Bereiche UNIX und E-Business-Infrastruktur spezialisiert. Wir bieten zudem perfekt auf die Kundenbedürfnisse zugeschnittene Security-Lösungen an – selbstverständlich produkt- und herstellerneutral.

## Unser Leistungsangebot

- Rechenzentrumsbetrieb (Betriebssysteme, Datenbanken, Webserver)
- Datensicherung
- Datensicherheit
- Datenverschlüsselung
- Virtual Private Networks (VPN)

## Kontakt

### Thinking Objects Software GmbH

Lilienthalstr. 2/1  
70825 Stuttgart-Korntal  
Germany

Tel.: +49.711.88770.400  
Fax: +49.711.88770.449  
Mail: [info@to.com](mailto:info@to.com)  
[www.to.com](http://www.to.com)